PACIFIC JOURNAL OF MATHEMATICS
Vol. 127, No. 1, 1987

EXPONENTIALS AND LOGARITHMS ON WITT RINGS

MURRAY MARSHALL

Suppose R is an Abstract Witt Ring in the terminology of Knebusch, Rosenberg, and Ware so $R = \mathbf{Z}[G]/K$ where G is Abelian and p-primary. Suppose further that G has exponent p and that, for all $x \in \mathbf{Z}[G]$, $x \in K$ implies $x^p/p \in K$. For example, this holds in the case where $p = 2$ and R is strongly representational. Let $\overline{M} = M/K$ be the fundamental ideal of R. Then a system of divided powers is defined on the torsion part of $\overline{M}$ and there is a well-behaved exponential map defined on the torsion part of $\overline{M}^2$. This yields a description of the multiplicative group of units of R in terms of the additive structure of $\overline{M}^2$.

If R is the Witt ring of bilinear forms over some field (or local or semi-local ring) in which 2 is a unit then R has certain rather special properties. For example, R is a strongly representational Witt ring in the terminology of [4] or [7]. However, for most of what is done here all one needs to know is that R has a particular sort of presentation as a quotient of an abelian group ring. Namely $R = \mathbf{Z}[G]/K$ where G is an abelian group of exponent 2 and K is generated as an ideal by some element $1 + e$, $e \in G$, together with certain elements of the form $(1 - g)(1 - h)$, $g, h \in G$; e.g. see [7]. The Witt ring of bilinear forms over a local or semi-local ring in which 2 is not a unit does not have quite such a nice presentation and the results proved here do not seem to apply in this case.

A much more general concept, namely that of an abstract Witt ring was introduced earlier in [5]. Fix a prime p and an abelian group G which is p-primary torsion and consider a ring of the form $R = \mathbf{Z}[G]/K$, K some ideal in $\mathbf{Z}[G]$. There are various ways of saying what it means for R to be an abstract Witt ring. One characterization is that R_{tor} (= the torsion part of R) is p-primary torsion. Denote by M the ideal of $\mathbf{Z}[G]$ generated by p and all elements $1 - g$, $g \in G$. This is the unique maximal ideal in $\mathbf{Z}[G]$ containing p. Also $M \supseteq K$ so we can form $\overline{M} := M/K$. There are only two possibilities: either (1) $R_{\text{tor}} = R$, $\overline{M}$ is the only prime ideal of R, so R is local with nilradical $\overline{M}$ or (2) $\mathrm{R}_{\text{tor}} \neq R$, $R_{\text{tor}} \subseteq \overline{M}$, and R_{tor} is the nilradical of R. Thus, in any case, one can say that $(\overline{M})_{\text{tor}} := \overline{M} \cap R_{\text{tor}}$ is the nilradical of R, although this statement by itself is probably a bit misleading.

In this paper we consider only the case where G has exponent p. The case of major interest, to the author at least, is $p = 2$, but it is hard to ignore the fact almost everthing goes over to the case of an odd prime. We consider abstract Witt rings which satisfy the additional special property:

$$(*) \qquad x \in K \Rightarrow \frac{x^p}{p} \in K.$$

This is pretty restrictive but it does include the case mentioned above where $p = 2$ and K is generated by an element $1 + e$, $e \in G$, and certain elements of the form $(1 - g)(1 - h)$, $g, h \in G$. It turns out that whenever $(*)$ holds then $(\overline{M})_{\text{tor}}$ has a system of divided powers $\gamma_n \colon (\overline{M})_{\text{tor}} \to R$, $n \geq 0$, in the sense of [**1**] (also see [**2**]). Basically, this just means that there are elements $\gamma_n(x)$ with all the formal properties of $x^n/n!$. Further, if $x \in (\overline{M}^2)_{\text{tor}} := \overline{M}^2 \cap R_{\text{tor}}$, then $\gamma_n(x) = 0$ for n sufficiently large. This allows the definition of $\exp(x)$, $\log(1 + x)$ for $x \in (\overline{M}^2)_{\text{tor}}$ and one can prove that

$$(\overline{M}^2)_{\text{tor}} \underset{\log}{\overset{\exp}{\rightleftarrows}} 1 + (\overline{M}^2)_{\text{tor}}$$

are group isomorphisms which are inverse to each other. These isomorphisms preserve the natural filtration, i.e. $\exp((\overline{M}^n)_{\text{tor}}) = 1 + (\overline{M}^n)_{\text{tor}}$ for all $n \geq 2$. Also, exp and log are independent of the particular presentation $R = \mathbf{Z}[G]/K$. Actually, if p is odd, one can do a bit better and prove that if $x \in (\mathbf{Z}p + \overline{M}^2)_{\text{tor}}$ then $\gamma_n(x) = 0$ for n sufficiently large so in this case we have inverse isomorphisms

$$(\mathbf{Z}p + \overline{M}^2)_{\text{tor}} \underset{\log}{\overset{\exp}{\rightleftarrows}} 1 + (\mathbf{Z}p + \overline{M}^2)_{\text{tor}}.$$

Denote by U the group of units of finite order in R. If $p = 2$ or 3 or if $R_{\text{tor}} = R$ then U is the full group of units of R [**5**]. Also, denote by $\overline{G}$ the image of G in R. Then it is possible to show, modifying slightly the proofs in [**5**], that

$$\begin{cases} U = (\pm\overline{G})(1 + (\overline{M}^2)_{\text{tor}}), & \text{if } p = 2, \\ U = (\pm\overline{G})\left(1 + (\mathbf{Z}p + \overline{M}^2)_{\text{tor}}\right), & \text{if } p \neq 2,\ R_{\text{tor}} \neq R. \end{cases}$$

There is an analogous result if $p \neq 2$, $R_{\text{tor}} = R$, but this is left to the main body of the paper. If reasonably mild restrictions are placed on K (restrictions that hold if $p = 2$ and K is generated by an element $e + 1$, $e \in G$, and elements $(1 - g)(1 - h)$, $g, h \in G$) then this product decomposition of U is in fact direct. In any case, this combines with the above mentioned results to give a more or less complete description of U in terms of the additive group $(\overline{M}^2)_{\text{tor}}$ if $p = 2$ (resp. in terms of the additive group $(\mathbf{Z}p + \overline{M}^2)_{\text{tor}}$ if p is odd).

In case $p = 2$ and R is strongly representational an additional refinement is possible. Let $\text{Ann}(2^k) := \{x \in R \mid 2^k x = 0\}$. Then using the abstract analogue of the annihilator theorem for Pfister forms given in [**4**], one can show that the ideal $\text{Ann}(2^k)$ has divided powers (if $2^k \neq 0$ in R) and consequently that exp and log induce inverse isomorphisms

$$\text{Ann}(2^k) \cap \overline{M}^2 \underset{\log}{\overset{\exp}{\rightleftarrows}} 1 + \text{Ann}(2^k) \cap \overline{M}^2$$

for all $k \geq 0$. In particular, for $x \in \overline{M}^2$ one has $(1 + x)^{2^k} = 1$ iff $2^k x = 0$.

1. Divided powers. Let A be a commutative ring with 1, I an ideal of A. Following [**1**] we say that I has *divided powers* if there exists a sequence of functions $\gamma_i \colon I \to A$, $i \geq 0$, satisfying

$$\gamma_0(x) = 1, \quad \gamma_1(x) = x, \quad \gamma_n(x) \in I \qquad \text{for all } n \geq 2, \tag{1}$$

$$\gamma_n(x + y) = \sum_{i=0}^{n} \gamma_i(x)\gamma_{n-i}(y), \tag{2}$$

$$\gamma_n(ax) = a^n \gamma_n(x), \tag{3}$$

$$\gamma_m(x)\gamma_n(x) = \frac{(m+n)!}{m!n!}\gamma_{m+n}(x), \quad \text{and} \tag{4}$$

$$\gamma_m(\gamma_n(x)) = \frac{(mn)!}{m!(n!)^m}\gamma_{mn}(x). \tag{5}$$

Here x, $y \in I$, $a \in A$, and m, $n \in \mathbf{N}$. Clearly (1) and (4) together imply that $n!\gamma_n(x) = x^n$. Thus, if A is a $\mathbf{Q}$-algebra, there is a unique system of divided powers on $I = A$ given by $\gamma_n(x) = x^n/n!$. More generally, if A is torsion free as an abelian group, then $A \hookrightarrow A \otimes \mathbf{Q}$ so divided powers on an ideal in A, if they exist, are unique and given by $\gamma_n(x) = x^n/n!$.

Fix a prime $p \in \mathbf{Z}$ and let $\mathbf{Z}_{(p)} \subseteq \mathbf{Q}$ denote the ring of p-adic integers. We are particularly interested, to begin with, in the case where A is a torsion free $\mathbf{Z}_{(p)}$-algebra. Recall if $n = \sum n_i p^i$ is the p-adic expansion of some fixed $n \geq 0$ (so $0 \leq n_i < p$) then p divides $n!$

$$v_p(n!) := \sum_{i \geq 0} n_i \left(\frac{p^i - 1}{p - 1}\right)$$

times. Thus $n!$ decomposes as

$$n! = n_* p^{v_p(n!)} = n_* \prod_{i \geq 0} \left(p^{(p^i - 1)/(p-1)}\right)^{n_i}$$

where n_* is relatively prime to p. Define $\gamma(x) = x^p/p$. Then by induction

$$\gamma^i(x) = \frac{x^{p^i}}{p^{(p^i-1)/(p-1)}}$$

where $\gamma^i := \gamma \circ \cdots \circ \gamma$ (i times). Also

$$\gamma_n(x) = \frac{x^n}{n!} = \frac{\prod_{i\geq 0}(x^{p^i})^{n_i}}{n_*\prod_{i\geq 0}\left(p^{(p^i-1)/(p-1)}\right)^{n_i}}$$

so we have the *decomposition formula*

$$\gamma_n(x) = \frac{1}{n_*}\prod_{i>0}(\gamma^i(x))^{n_i}$$

Thus γ_n is completely described in terms of γ (also see [**1**]). Observe, since n_* is relatively prime to p, $1/n_*$ makes sense in A if A is a $\mathbf{Z}_{(p)}$-algebra.

Now suppose we go to the set-up described in the introduction. That is, G is a group of exponent p, $R = \mathbf{Z}[G]/K$ is an abstract Witt ring, etc. We attempt to put divided powers on the ideal $(\overline{M})_{\text{tor}} \subseteq R$. Consider $\mathbf{Z}[G] \subseteq \mathbf{Z}_{(p)}[G] \subseteq \mathbf{Q}[G]$ and denote by $M_{(p)} := M \otimes \mathbf{Z}_{(p)}$ the ideal in $\mathbf{Z}_{(p)}[G]$ generated by $M \subseteq \mathbf{Z}[G]$.

(1.1) LEMMA. (1) *If $x \in M$ then $\gamma(x) \in M$.*

(2) *The ideal $M_{(p)} \subseteq \mathbf{Z}_{(p)}[G]$ has divided powers (necessarily unique).*

Proof. Elements of $M_{(p)}$ have the form $x = y/l$ with $y \in M$, l an integer relatively prime to p. Thus, if we assume (1) then it follows that $x \in M_{(p)} \Rightarrow x^p/p \in M_{(p)}$. This, together with the decomposition formula for $\gamma_n(x)$ shows that $\gamma_n(x) \in M_{(p)}$ for all $x \in M_{(p)}$, $n \geq 1$, and completes the proof of (2). To prove (1) note the identities:

$$\gamma(x+y) = \gamma(x) + \gamma(y) + \sum_{i=1}^{p-1}\frac{(p-1)!}{i!(p-i)!}x^i y^{p-i}$$

and

$$\gamma(ax) = a^p\gamma(x).$$

These show that the set $\{x \in M \mid \gamma(x) \in M\}$ is an ideal in $\mathbf{Z}[G]$. Thus it is enough to check the result for generators of M. Recall that M is generated by p and all elements $1 - g$, $g \in G$, $g \neq 1$. Now $\gamma(p) = p^p/p = p^{p-1} \in M$. Also we have a polynomial identity

$$(1-x)^p - (1-x^p) = p\phi(x)(1-x)$$

where $\phi(x)$ has integer coefficients. Substituting g for x and using $g^p = 1$, this yields $(1-g)^p = p\phi(g)(1-g)$, so $\gamma(1-g) = \phi(g)(1-g) \in M$. [Note: if $p = 2$ these read $\gamma(2) = 2$, $\gamma(1-g) = 1-g$.] □

Now since R is a Witt ring, R_{tor} is p-primary torsion so $R \hookrightarrow R_{(p)}$ where $R_{(p)} := R \otimes \mathbf{Z}_{(p)}$. This means that $K = K_{(p)} \cap \mathbf{Z}[G]$.

(1.2) LEMMA. *The following are equivalent*:
(1) *for all* $x \in \mathbf{Z}[G]$, $x \in K \Rightarrow x^p/p \in K$,
(2) *the ideal* $K_{(p)} \subseteq \mathbf{Z}_{(p)}[G]$ *has divided powers.*

Proof. If (1) holds then, as in the previous proof, $x \in K_{(p)} \Rightarrow x^p/p \in K_{(p)}$. This, plus the decomposition formula for $\gamma_n(x)$ shows that $\gamma_n(x) \in K_{(p)}$ holds for all $x \in K_{(p)}$ and all $n \geq 1$ so $K_{(p)}$ has divided powers. Conversely if (2) holds and $x \in K$, then $x^p/p = (p-1)!\gamma_p(x) \in K_{(p)}$ but also $K \subseteq M$, so $x^p/p \in M \subseteq \mathbf{Z}[G]$. Thus $x^p/p \in K_{(p)} \cap \mathbf{Z}[G] = K$.

(1.3) PROPOSITION. *Suppose K satisfies condition* (1) *of* (1.2). *Then the divided powers on $M_{(p)} \subseteq \mathbf{Z}_{(p)}[G]$ induce divided powers on $\overline{M}_{(p)} \subseteq R_{(p)}$ and on $(\overline{M})_{\mathrm{tor}} \subseteq R$. (Here, notation is as in the introduction.)*

Proof. Consider the diagram

$$\begin{tikzcd} \mathbf{Z}_{(p)}[G] \arrow[r, hook] \arrow[d] & \mathbf{Q}[G] \\ R \arrow[r, hook] & R_{(p)}. \end{tikzcd}$$

We know $M_{(p)} \subseteq \mathbf{Z}_{(p)}[G]$ has divided powers by (1.1) and, by (1.2), $\gamma_n(x) \in K_{(p)}$ holds for all $x \in K_{(p)}$, $n \geq 1$. Suppose $\bar{x} \in R_{(p)}$ denotes the image of $x \in \mathbf{Z}_{(p)}[G]$. Then there are induced divided powers on the image of $M_{(p)}$ in $R_{(p)}$ given by $\gamma_n(\bar{x}) = \overline{\gamma_n(x)}$. Moreover, this image is just $\overline{M}_{(p)}$. This does not quite allow us to pull the divided powers back to $\overline{M}$ since $\overline{M} \hookrightarrow \overline{M}_{(p)}$ may not be surjective. However, $(\overline{M})_{\mathrm{tor}}$ is p-primary torsion, so the embedding $(\overline{M})_{\mathrm{tor}} \to ((\overline{M})_{\mathrm{tor}})_{(p)}$ is surjective. Thus to show we have divided powers on the ideal $(\overline{M})_{\mathrm{tor}} \subseteq R$ it suffices to check that the divided powers on $(\overline{M})_{(p)}$ induce divided powers on $((\overline{M})_{\mathrm{tor}})_{(p)}$. This just involves checking that if $x \in (\overline{M})_{(p)}$ is torsion, then so is $\gamma_n(x)$ if $n \geq 1$. But this is clear since if $p^k x = 0$, then $p^{nk}\gamma_n(x) = \gamma_n(p^k x) = \gamma_n(0) = 0$. □

(1.4) REMARK. Since we know $x \in M \Rightarrow \gamma(x) \in M$ there is nothing very mysterious about the divided powers γ_n: $(\overline{M})_{\mathrm{tor}} \to R$. Suppose $\bar{x} \in \overline{M}$ denotes the image of $x \in M$ and define $\gamma(\bar{x}) := \overline{\gamma(x)} \in \overline{M}$. We have the decomposition formula

$$\gamma_n(\bar{x}) = \frac{1}{n_*}\prod_{i\geq 0}(\gamma^i(\bar{x}))^{n_i}.$$

Now $\prod_{i\geq 0}(\gamma^i(\bar{x}))^{n_i}$ is a well defined element of $\overline{M}$ (at least if $n \geq 1$) and n_* is relatively prime to p, so $\gamma_n(\bar{x})$ makes sense in $(\overline{M})_{(p)}$. Also, if $\bar{x} \in (\overline{M})_{\text{tor}}$, then $\gamma(\bar{x}) \in (\overline{M})_{\text{tor}}$ and consequently, $\prod_{i\geq 0}(\gamma^i(\bar{x}))^{n_i} \in (\overline{M})_{\text{tor}}$. Since the torsion is p-primary, this allows interpreting $\gamma_n(\bar{x})$ as an element of $(\overline{M})_{\text{tor}}$ in this case.

(1.5) Examples. (1) Suppose $p = 2$ and K has a system of generators consisting of an element $1 + e$, $e \in G$, and certain elements of the form $(1 - g)(1 - h)$, $g, h \in G$. By results in [5], R is an abstract Witt ring in this case. Also K satisfies $x \in K \Rightarrow x^2/2 \in K$ so (1.3) applies. Note: To check the condition $x \in K \Rightarrow x^2/2 \in K$ it is enough to check it on the generators for K but here it is clear since

$$\frac{(1+e)^2}{2} = \frac{1+2e+e^2}{2} = \frac{1+2e+1}{2} = \frac{2+2e}{2} = 1 + e$$

and

$$\frac{(1-g)^2(1-h)^2}{2} = \frac{2(1-g)2(1-h)}{2} = 2(1-g)(1-h)$$

(2) Here are two trivial examples: Take G to be cyclic of order p generated by g say. Then $\mathbf{Z}/\mathbf{Z}p^k$ is an abstract Witt ring for G by taking K the ideal generated by p^k and $1 - g$. This clearly satisfies $x \in K \Rightarrow x^p/p \in K$ so we have divided powers on $\mathbf{Z}p/p^k$. For the second example let $\mathbf{Z}[\delta]$ denote the rings of algebraic integers generated by δ, a primitive pth root of unity. This is an abstract Witt ring for G taking K to be the ideal generated by the element $1 + g + \cdots + g^{p-1}$. We have a polynomial identity

$$(1 + x + \cdots + x^{p-1})^p - p^{p-1}(1 + x + \cdots + x^{p-1}) = (1 - x^p)\psi(x)$$

for some polynomial $\psi(x)$ with integer coefficients. Thus

$$\gamma(1 + g + \cdots + g^{p-1}) = p^{p-2}(1 + g + \cdots + g^{p-1}).$$

Thus we have divided powers on the ideal in $\mathbf{Z}[\delta]$ generated by $1 - \delta$.

2. exp and log. Assume the set-up of §1 with K satisfying $x \in K \Rightarrow x^p/p \in K$. Thus we have divided powers on $M_{(p)} \subseteq \mathbf{Z}_{(p)}[G]$, on $\overline{M}_{(p)} \subseteq R_{(p)}$, and on $(\overline{M})_{\text{tor}} \subseteq R$. Suppose $x = x_1 \cdots x_k$, $x_i \in M_{(p)}$. Then $\gamma_n(x) = (x_1 \cdots x_{k-1})^n\gamma_n(x_k) \in M^{n(k-1)+1}$. Using the expansion for $\gamma_n(x+y)$ yields $\gamma_n(M^k_{(p)}) \subseteq M^{n(k-1)+1}_{(p)}$. Pushing this down via $\mathbf{Z}_{(p)}[G] \to R_{(p)}$ and back via $R \hookrightarrow R_{(p)}$ this yields $\gamma_n(\overline{M}^k_{(p)}) \subseteq \overline{M}^{n(k-1)+1}_{(p)}$ and $\gamma_n((\overline{M}^k)_{\text{tor}}) \subseteq (\overline{M}^{n(k-1)+1})_{\text{tor}}$. This is not too good if $k=1$ but for $k=2$ it yields $\gamma_n((\overline{M}^2)_{\text{tor}}) \subseteq (\overline{M}^{n+1})_{\text{tor}}$. We use this estimate to prove the following:

(2.1) PROPOSITION. *For any* $x \in (\overline{M}^2)_{\text{tor}}$, $\gamma_n(x) = 0$ *if* n *is sufficiently large.*

Proof. First suppose G is finite. Then we *claim* $(\overline{M}^n)_{\text{tor}} = 0$ if n is sufficiently large. Since $\gamma_n((\overline{M}^2)_{\text{tor}}) \subseteq (\overline{M}^{n+1})_{\text{tor}}$, this will complete the proof in this case. Since G is finite, R and R_{tor} are finitely generated abelian groups. Since R_{tor} is torsion, R_{tor} is actually finite so there is some large k such that $p^k R_{\text{tor}} = 0$. Any element of $\overline{M}^n$ is a finite sum of products of the form $m(1-\bar{g}_1)\cdots(1-\bar{g}_s)p^{n-s}$. Here $m \in \mathbf{Z}$, $g_i \in G$, and $\bar{g}$ denotes the image in R of $g \in G$. If s is large there are lots of repeated factors $1-\bar{g}$ in this product. Since $(1-\bar{g})^p = p\phi(\bar{g})(1-\bar{g})$ (see the proof of (1.1)) it follows that if n is large enough, then $\overline{M}^n \subseteq p^k R$, so $(\overline{M}^n)_{\text{tor}} \subseteq p^k R \cap R_{\text{tor}} = p^k R_{\text{tor}} = 0$.

To do the general case suppose $x \in (\overline{M}^2)_{\text{tor}}$, say

$$x = np^2 + \sum_i n_i p(1-\bar{g}_i) + \sum_j m_j(1-\bar{h}_j)(1-\bar{h}'_j)$$

n, n_i, $m_j \in \mathbf{Z}$ and g_i, h_j, $h'_j \in G$. Let H be the subgroup of G generated by the elements g_i, h_j, h'_j. This is a finite group. Let $S = \mathbf{Z}[H]/L$ where $L = K \cap \mathbf{Z}[H]$. Also, let $N = M \cap \mathbf{Z}[H]$, so N is the ideal of $\mathbf{Z}[H]$ generated by p and the elements $1-g$, $g \in H$. S is an abstract Witt ring for H (as pointed out in [5]). Also, if $y \in L$, then $y^p/p \in K$ (since $L \subseteq K$) but also $L \subseteq N$ so $y^p/p \in N \subseteq \mathbf{Z}[H]$ as in (1.1). Thus $y \in L \Rightarrow y^p/p \in L$. Finally, by choice of H, $x \in \overline{N}^2$ and since $S \hookrightarrow R$, x is torsion in S, so $x \in (\overline{N}^2)_{\text{tor}}$. Since the divided powers on S are just those induced from R, we are done by the finite case. □

If p is odd we can make a slight improvement in (2.1):

(2.2) PROPOSITION. *Suppose* p *is odd. Then for every* $x \in (\mathbf{Z}p + \overline{M}^2)_{\text{tor}}$, $\gamma_n(x) = 0$ *if* n *is sufficiently large.*

Proof. One has the estimate $\gamma_n(p) = p^n/n! \equiv 0 \bmod p^l$ where

$$l = n - \sum_{i\geq 0} n_i\left(\frac{p^i-1}{p-1}\right) = \frac{p-2}{p-1}n + \sum_{i>0} n_i \geq \frac{1}{2}n + 1.$$

Here, of course, $n = \Sigma n_i p^i$ is the p-adic expansion. Using this and expanding $\gamma_n(mp + x)$, $m \in \mathbf{Z}_{(p)}$, $x \in M^2_{(p)}$, we obtain

$$\gamma_n\left(\mathbf{Z}_{(p)}p + M^2_{(p)}\right) \subseteq M_{(p)}^{[(n+1)/2]+1}$$

where [ ] denotes the greatest integer function. Pulling this back down to R yields

$$\gamma_n\left((\mathbf{Z}p + \overline{M}^2)_{\text{tor}}\right) \subseteq \left(\overline{M}^{[(n+1)/2]+1}\right)_{\text{tor}}.$$

Now the same argument used in (2.1) shows that if $x \in (\mathbf{Z}p + \overline{M}^2)_{\text{tor}}$ then $\gamma_n(x) = 0$ for n sufficiently large. □

In view of (2.1) we can now define

$$\begin{cases} \exp\colon & (\overline{M}^2)_{\text{tor}} \to 1 + (\overline{M}^2)_{\text{tor}} \\ \log\colon & 1 + (\overline{M}^2)_{\text{tor}} \to (\overline{M}^2)_{\text{tor}} \end{cases}$$

by $\exp(x) := \Sigma_{i \geq 0}\gamma_i(x)$, $\log(1 + x) = \Sigma_{i \geq 1}(-1)^{i+1}(i - 1)!\gamma_i(x)$, for $x \in (\overline{M}^2)_{\text{tor}}$. If $p \neq 2$ we can extend this slightly and define

$$\begin{cases} \exp\colon & (\mathbf{Z}p + \overline{M}^2)_{\text{tor}} \to 1 + (\mathbf{Z}p + \overline{M}^2)_{\text{tor}} \\ \log\colon & 1 + (\mathbf{Z}p + \overline{M}^2)_{\text{tor}} \to (\mathbf{Z}p + \overline{M}^2)_{\text{tor}} \end{cases}$$

using the same formulas, but with $x \in (\mathbf{Z}p + \overline{M}^2)_{\text{tor}}$. Since $(\overline{M})_{\text{tor}}$ is the nilradical of R, $1 + (\overline{M}^2)_{\text{tor}}$ and $1 + (\mathbf{Z}p + \overline{M}^2)_{\text{tor}}$ are subgroups of the unit group of R.

(2.3) PROPOSITION. exp *and* log *so defined are group isomorphisms and* log = exp^{-1}.

Proof. The fact that exp is a homomorphism follows easily from the formula $\gamma_n(x + y) = \Sigma_{i=0}^n \gamma_k(x)\gamma_{n-i}(y)$. To show exp and log are inverse to each other we want to show

$$\begin{cases} \sum_{i=1}^{k} (-1)^{i+1}(i-1)!\gamma_i\left(\sum_{j=1}^{k}\gamma_j(x)\right) = x, \\ \sum_{j=1}^{k}\gamma_j\left(\sum_{i=1}^{k}(-1)^{i+1}(i-1)!\gamma_i(x)\right) = x \end{cases}$$

where $x \in (\overline{M}^2)_{\text{tor}}$ if $p = 2$ (resp. $x \in (\mathbf{Z}p + \overline{M}^2)_{\text{tor}}$ if p is odd) and k is so large that $\gamma_l(x) = 0$ for $l \geq k$. Undoubtably these identities follow from the formal properties of divided powers given in §1. However one can also argue as follows: Let $\mathbf{Z}_{(p)}\langle t\rangle$ denote the free divided power algebra in one variable t over $\mathbf{Z}_{(p)}$ (see [1]). This is the $\mathbf{Z}_{(p)}$-subalgebra of the polynomial ring $\mathbf{Q}[t]$ with $\mathbf{Z}_{(p)}$-basis consisting of $1, t, \dots, t^n/n!, \dots$. It is well-known that the ideal in $\mathbf{Z}_{(p)}\langle t\rangle$ generated by the elements $t^n/n!$, $n \geq 1$ is a divided power ideal and that $\mathbf{Z}_{(p)}\langle t\rangle$ has the following universal property: Suppose A is any $\mathbf{Z}_{(p)}$-algebra and $x \in I$ where $I \subseteq A$ is an ideal with divided powers. Then there is a unique algebra homomorphism ϕ: $\mathbf{Z}_{(p)}\langle t\rangle \to A$ with $\phi(t) = x$ satisfying $\phi(\gamma_n(y)) = \gamma_n(\phi(y))$ for all $y \in \mathbf{Z}_{(p)}\langle t\rangle$ without constant term. Now up in $\mathbf{Z}_{(p)}\langle t\rangle$ we know for sure that the congruences

$$\begin{cases} \displaystyle\sum_{i=1}^{k} (-1)^{i+1}(i-1)!\gamma_i\left(\sum_{j=1}^{k}\gamma_j(t)\right) \equiv t, \\ \displaystyle\sum_{j=1}^{k} \gamma_j\left(\sum_{i=1}^{k}(-1)^{i+1}(i-1)!\gamma_i(t)\right) \equiv t \end{cases}$$

hold modulo the ideal of terms of degree $\geq k$. Pushing these congruences down by the universal mapping ϕ: $\mathbf{Z}_{(p)}\langle t\rangle \to R$ with $\phi(t) = x$ yields the corresponding identities in R.

(2.4) PROPOSITION. exp *and* log *as defined do not depend on the particular presentation* $R = \mathbf{Z}[G]/K$.

Proof. Suppose there is another presentation $R = \mathbf{Z}[G']/K'$ inducing another system of divided powers δ_n, $n \geq 0$. To avoid the trivial case exp: $\{0\} \to \{1\}$, log: $\{1\} \to \{0\}$ which is obviously unique, we can assume $R_{\text{tor}} \neq 0$. Since R_{tor} is p-primary torsion, this means that p is independent of the presentation. $\overline{M}$ is characterized as the unique maximum ideal in R containing p (see [5]) and as such is also independent of the presentation. Also, for x, $y \in \overline{M}$ (or $\overline{M}_{(p)}$), $\gamma_n(xy) = x^n\gamma_n(y) = n!\delta_n(x)\gamma_n(y) = y^n\delta_n(x) = \delta_n(xy)$. This proves that $\gamma_n = \delta_n$ on $\overline{M}^2$ and hence on $(\overline{M}^2)_{\text{tor}}$. This completes the proof if $p = 2$. If $p \neq 2$ we also have $\gamma_n(p) = p^n/n! = \delta_n(p)$ so $\gamma_n = \delta_n$ on $\mathbf{Z}p + \overline{M}^2$ and hence on $(\mathbf{Z}p + \overline{M}^2)_{\text{tor}}$. This completes the proof if $p \neq 2$. □

Suppose J is some ideal of R, $J \subseteq (\overline{M}^2)_{\text{tor}}$ if $p = 2$ (resp. $J \subseteq (\mathbf{Z}p + \overline{M}^2)_{\text{tor}}$ if $p \neq 2$). Then for exp and log to induce inverse isomorphisms exp: $J \to 1 + J$, log: $1 + J \to J$, it is clearly sufficient that J is a divided power ideal, i.e. that $\gamma_n(J) \subseteq J$ for all $n \geq 1$. Examples of such ideals include the ideals $(\overline{M}^j)_{\text{tor}}$ if $j \geq 2$. This follows from the estimate given earlier, namely that $\gamma_n((\overline{M}^j)_{\text{tor}}) \subseteq (\overline{M}^{(j-1)n+1})_{\text{tor}}$. Of course, if I, J have divided powers then so do $I + J$, $I \cap J$ and IL for any ideal $L \subseteq R$.

A more interesting class of ideals are the ideals $\overline{M}^2 \cap \text{Ann}(p^k)$ where $\text{Ann}(p^k) := \{x \in R \mid p^k x = 0\}$. The question here is: does $x \in \overline{M}^2$, $p^i x = 0$, imply $p^k \gamma_n(x) = 0$ for $n \geq 1$? Equivalently, by the decomposition formula for $\gamma_n(x)$, is it true that $x \in \overline{M}^2$, $p^k x = 0$, implies $p^k \gamma(x) = 0$? [Note: $p^k \gamma(x) = p^{k-1}(p\gamma(x)) = p^{k-1}x^p$.] It turns out that this is not true in general (see example (2.7) below). However, one does have the following result which is of interest from the point of quadratic form theory:

(2.5) PROPOSITION. *Suppose $p = 2$ and R is strongly representational in the sense of* [**4**] *or* [**7**]. *Then* $\text{Ann}(2^k)$ *has divided powers if* $2^k \neq 0$. *Consequently, we have induced isomorphisms*

$$\overline{M}^i \cap \text{ann}(2^k) \underset{\log}{\overset{\exp}{\rightleftarrows}} 1 + \overline{M}^i \cap \text{Ann}(2^k)$$

for all $i \geq 2$ *and all* $k \geq 0$. *Also, if* $x \in \overline{M}^2$, *then* $(1 + x)^{2^k} = 1$ *iff* $2^k x = 0$.

Proof. For strongly representational Witt rings one has an annihilator theorem for Pfister forms [**4**] generalizing a well-known result for quadratic forms over fields, e.g. see [**6**, p. 71]. Applying this to the Pfister element $2^k = (1 + 1) \cdots (1 + 1)$ it follows that if $2^k x = 0$, then x decomposes as $x = \sum x_i(1 - \bar{s}_i)$, $x_i \in R$, $\bar{s}_i \in \overline{G}(2^k)$, where $\overline{G}(2^k) := \{\bar{s} \in \overline{G} \mid 2^k \bar{s} = 2^k\}$. ($\overline{G}$ just denotes the image of G in R via $\mathbf{Z}[G] \to R$.) This says precisely that the elements $1 - \bar{s}$, $\bar{s} \in \overline{G}(2^k)$, generate $\text{Ann}(2^k)$ as an ideal. Now $\gamma(1 - \bar{s}) = 1 - \bar{s}$ so this shows $\gamma(\text{Ann}(2^k)) \subseteq \text{Ann}(2^k)$ and hence that $\text{Ann}(2^k)$ has divided powers. The second assertion is now immediate.

Now suppose $x \in \overline{M}^2$. First suppose $(1 + x)^{2^k} = 1$. Then $x \in (\overline{M}^2)_{\text{tor}}$. This is pretty well-known for strongly representational Witt rings but for the proof the reader may wish to refer to (3.1) in the next section. Let $y = \log(1 + x)$. Then $2^k y = 0$, so $2^k \gamma_n(y) = 0$ for all $n \geq 1$. Thus $x = \exp(y) - 1 = \sum_{n \geq 1} \gamma_n(y)$ also satisfies $2^k x = 0$. Next suppose $2^k x = 0$. Then again $2^k \gamma_n(x) = 0$ for all $n \geq 1$, so $y = \log(1 + x) = \sum_{n \geq 1}(-1)^{n+1}(n - 1)!\gamma_n(x)$ also satisfies $2^k y = 0$. But this means $(1 + x)^{2^k} = 1$.

(2.6) REMARK. If R is strongly representational, $2^k \neq 0$ in R, then $\overline{M}^2 \cap \text{Ann}(2^k) = \overline{M}\,\text{Ann}(2^k)$. The proof of this goes through using the argument in [**3**] as soon as one knows the annihilator theorem for 2^k. This implies, in particular, that $(\overline{M}^2)_{\text{tor}} = (\overline{M})(R_{\text{tor}})$ if $R_{\text{tor}} \neq R$. If R is of elementary type (see [7]) then one actually has $\overline{M}^j \cap \operatorname{Ann}(2^k) = \overline{M}^{j-1}\operatorname{Ann}(2^k)$ for all $j \geq 2$ (provided of course that $2^k \neq 0$ in R).

The question of whether or not the conclusion of (2.5) holds for any Witt ring with $p = 2$ and K generated by an element $1 + e$, $e \in G$, and certain elements $(1 - g)(1 - h)$, g, $h \in G$, has not been resolved. The author would guess that it fails in this more general case. Anyway, it is not valid for all Witt rings, as the following example shows.

(2.7) EXAMPLE. Here is an example of a Witt ring with divided powers, $p = 2$, with $\bar{x} \in \overline{M}^2$, $2\bar{x} = 0$, but $\bar{x}^2 = 2\gamma(\bar{x}) \neq 0$. Take $|G| = 16$, G generated by g_1, g_2, h_1, h_2 and take

$$x = (1 - g_1)(1 - g_2) + (1 - h_1)(1 - h_2).$$

Take K to be the ideal in $\mathbf{Z}[G]$ generated by x and 8. Then one can check that $4(1 - g_1)(1 - g_2)$ does not lie in this ideal. This is a bit tedious so the details are omitted. Since $x^2/2 \equiv 4(1 - g_1)(1 - g_2) \pmod{K}$ this shows that $x^2/2 \notin K$, so divided powers are not defined. This is not quite what we want. However, suppose instead we take K to be the ideal generated by $2x$ and 16. Then divided powers are defined (since $(2x)^2/2 = 2x^2 \in K$) and now, of course, $8(1 - g_1)(1 - g_2)$ does not lie in K. Since $x^2 \equiv 8(1 - g_1)(1 - g_2) \pmod{K}$, this proves the required example. Taking this a little further one sees that $\gamma_n(\bar{x}) = 0$ if $n \geq 3$ so $\exp(\bar{x}) = 1 + \bar{x} + \gamma(\bar{x})$, $\log(1 + \bar{x}) = \bar{x} - \gamma(\bar{x})$. Thus $1 + \bar{x}$ has multiplicative order 4 although $\bar{x}$ only has additive order 2. Also, if $\bar{y} := \bar{x} + \gamma(\bar{x})$, then $1 + \bar{y}$ has multiplicative order 2 but $\bar{y}$ itself has additive order 4.

3. Units of finite order.

U denotes the group of units of finite order in R. In this section we develop a little of the structure of U. This is done in [5] where it is shown, for example, that $U = (\pm\overline{G})(1 + (\overline{M})_{\text{tor}})$ if $R_{\text{tor}} \neq R$. Unfortunately, the results in [5] are not quite in the form required here since we want to relate U to $1 + (\overline{M}^2)_{\text{tor}}$ if $p = 2$ (resp. to $1 + (\mathbf{Z}p + \overline{M}^2)_{\text{tor}}$ if p is odd). It should be emphasized that the material here is quite general, i.e., it does not require any special assumption that divided powers are defined.

We need a little more notation. Let I_G denote the ideal in $\mathbf{Z}[G]$ generated by the elements $1 - g$, $g \in G$. It is important to understand the relationship between I_G and M: We have $\mathbf{Z}[G] = \mathbf{Z} \oplus I_G$ and $M = \mathbf{Z}p \oplus I_G$. Also, the map $\Sigma_g n_g(1 - g) \to \Pi_g g^{n_g}$ induces a group isomorphism $I_G/I_G^2 \cong G$ with inverse $g \mapsto 1 - g + I_G^2$. This is well-known. In particular, since G has exponent p, this implies that $pI_G \subseteq I_G^2$ so $M^2 = \mathbf{Z}p^2 \oplus I_G^2$ and $\mathbf{Z}p + M^2 = \mathbf{Z}p \oplus I_G^2$.

(3.1) PROPOSITION. *Suppose* $z \in M^2$ *if* $p = 2$ (*resp.* $z \in Zp + M^2$ *if* p *is odd*). *Then* $1 + \bar{z}$ *is a unit of finite order in* R *iff* $\bar{z} \in R_{\text{tor}}$.

Proof. If $\bar{z} \in R_{\text{tor}}$ then $1 + \bar{z}$ is a unit of finite (p-power) order by [**5**, 3.21(i)]. Now assume that $1 + \bar{z}$ is a unit of finite order. We want to show that $\bar{z}$ is torsion. This is trivial if $R_{\text{tor}} = R$ so assume $R_{\text{tor}} \neq R$. Let ϕ: $\mathbf{Z}[G] \to A$ be any ring homomorphism with $K \subseteq \ker(\phi)$ where A denotes the ring of algebraic integers $\mathbf{Z}[\delta]$, δ a primitive pth root of unity. Let $\pi = 1 - \delta$ so $A\pi$ is prime in A and $A\pi \cap \mathbf{Z} = \mathbf{Z}p$. By assumption $\phi(1 + z) = 1 + \phi(z)$ is a unit of finite order in A and hence has the form $\varepsilon\delta^i$, $\varepsilon = \pm 1$, $0 \leq i < p$. Also, it is clear that $\phi(I_G) \subseteq A\pi$ so $\phi(z) \in A\pi^2$. [Note: $p \in A\pi^{p-1}$, so $p \in A\pi^2$ if $p \neq 2$.] Thus $\varepsilon\delta^i \equiv 1 \pmod{A\pi^2}$. This forces $\varepsilon\delta^i = 1$ so $\phi(z) = 0$. Since this holds for any such ϕ, $\bar{z} \in R_{\text{tor}}$ by results in [**5**]. □

The case where $p \neq 2$ and $R_{\text{tor}} = R$ is a bit special. In this case R has characteristic p^k for some $k \geq 1$ so $\mathbf{Z}/p^k\mathbf{Z} \hookrightarrow R$. The groups of units of $\mathbf{Z}/p^k\mathbf{Z}$ is cyclic of order $(p - 1)p^{k-1}$. In this special case we fix a generator ω for the cyclic group of units of order $p - 1$ in $\mathbf{Z}/p^k\mathbf{Z}$.

(3.2) PROPOSITION. *Every* $\bar{u} \in U$ *is expressible in the form* $\bar{u} = \varepsilon \cdot \bar{g}(1 + \bar{z})$ *where* $\bar{g} \in \bar{G}$, $\bar{z} \in (\overline{M^2})_{\text{tor}}$ *if* $p = 2$ (*resp.* $\bar{z} \in (\overline{\mathbf{Z}p + M^2})_{\text{tor}}$ *if* p *is odd*), $\varepsilon = \pm 1$ *if* $p = 2$ *or if* $R_{\text{tor}} \neq R$ (*resp.* $\varepsilon = \omega^i$ *for some* i, $0 \leq i < p - 1$, *if* $p \neq 2$ *and* $R_{\text{tor}} = R$). *Conversely, every* $\bar{u} \in R$ *of this form is a unit of finite order.*

Proof. The last assertion is immediate from (3.1). To prove the first assertion suppose $u \in \mathbf{Z}[G]$ is such that $\bar{u} \in R$ is a unit of finite order. Decompose u as $u = n - x$ with $n \in \mathbf{Z}$, $x \in I_G$. The first step is to reduce the case where $n = 1 + 4l$ if $p = 2$ (resp. $n = 1 + pl$ if p is odd). First suppose $p = 2$. Since $\bar{u}$ is a unit, $u \notin M$, so n is odd and hence $n \equiv \pm 1 \pmod 4$. Thus, replacing u by $-u$, if necessary, we have $n \equiv 1 \pmod 4$. Next suppose $p \neq 2$, $R_{\text{tor}} = R$. Then replacing u by $\omega^i u$ for some i, $0 \leq i \geq p - 1$, we can assume $n \equiv 1 \pmod p$. Finally, suppose $p \neq 2$, $R_{\text{tor}} \neq R$. Then by [**5**] there is a homomorphism ϕ: $\mathbf{Z}[G] \to A$, notation as in the proof of (1.1) with $K \subseteq \ker(\phi)$. Then $\phi(u) = \varepsilon\delta^i$, $\varepsilon = \pm 1$, $0 \leq i < p$, and $\phi(x) \in A\pi$, so $n \equiv \varepsilon\delta^i \pmod{A\pi}$. Since $\delta^i \equiv 1 \pmod{A\pi}$ this implies $n \equiv \varepsilon \pmod{A\pi}$ and hence $n \equiv \varepsilon \pmod p$. Thus, replacing u by $-u$ if necessary, we can assume $n \equiv 1 \pmod p$. This completes the first step.

Now decompose x as $x = (1 - g) + y$, $g \in G$, $y \in I_G^2$. Since $n = 1 + lp$ if p is odd (resp. $n = 1 + 4l$ if $p = 2$) and $u = n - x$, this yields (if p is odd)

$$u = 1 + pl - (1 - g) - y = g + pl - y,$$

so

$$\begin{aligned} g^{-1}u &= 1 + plg^{-1} - yg^{-1} \\ &= 1 + pl - (1 - g^{-1})pl - yg^{-1} \in 1 + \mathbf{Z}p + M^2. \end{aligned}$$

Similarly, if $p = 2$, $u = g + 4l - y$ so $g^{-1}u = 1 + 4lg^{-1} - yg^{-1} \in 1 + M^2$. Thus, replacing u by $g^{-1}u$ we can assume u has the form $u = 1 + z$ where $z \in M^2$ if $p = 2$ (resp. $z \in \mathbf{Z}p + M^2$ if p is odd). The result now follows from (3.1). □

If K is reasonably well behaved then it turns out that the product decomposition in (3.2) is direct and moreover that the homomorphism $G \to \overline{G}$ is an isomorphism. Before giving this result note, if p is odd, then in the decomposition $\bar{u} = \varepsilon \cdot \bar{g}(1 + \bar{z})$, ε has order relatively prime to p whereas $\bar{g}(1 + \bar{z})$ has p-power order by [5, 3.21(i)]. Thus in checking the directness the product in this case we can safely ignore the first factor.

(3.3) Proposition. (1) *For p odd, if $K \subseteq \mathbf{Z}p + M^2$ then $G \to \overline{G}$ is an isomorphism and the product $(\overline{G})(1 + (\mathbf{Z}p + \overline{M}^2)_{\text{tor}})$ is direct.*

(2) *For $p = 2$, if either $K \subseteq M^2$ or K is generated by certain elements of M^2 together with an element $1 + e$, $e \in G$, then $G \to \overline{G}$ is an isomorphism and the product $(\pm \overline{G})(1 + (\overline{M}^2)_{\text{tor}})$ is direct.*

Proof. Assume p is odd, $K \subseteq \mathbf{Z}p + M^2$. Suppose $g \in G$ and $\bar{g} \in 1 + (\mathbf{Z}p + \overline{M}^2)$. Then $1 - g \in \mathbf{Z}p + M^2 + K = \mathbf{Z}p + M^2 = \mathbf{Z}p \oplus I_G^2$. Thus $1 - g \in I_G^2$ so $g = 1$. This proves (1).

Now assume $p = 2$, $K \subseteq M^2$. Suppose $g \in G$ and $\pm\bar{g} \in 1 + \overline{M}^2$. Then $\pm g \in 1 + M^2 = (1 + 4\mathbf{Z}) \oplus I_G^2$. If the sign is $-$, then $1 - g \in (2 + 4\mathbf{Z}) \oplus I_G^2$ which is impossible. Thus the sign is $+$ and $1 - g \in 4\mathbf{Z} \oplus I_G^2$. Consequently $1 - g \in I_G^2$ so $g = 1$. Finally, assume $p = 2$ and that K is generated by elements from M^2 and an element $1 + e$, $e \in G$. Thus $\bar{e} = -1$ so $\pm\overline{G} = \overline{G}$. Suppose $g \in G$, $\bar{g} \in 1 + \overline{M}^2$. Thus $g \in 1 + M^2 + K$. Since $(1 - h)(1 + e) = (1 - h)(1 - eh) \in I_G^2$ for any $h \in G$, this yields $g = 1 + n(1 + e) + 4k + y$, n, $k \in \mathbf{Z}$, $y \in I_G^2$. This can be rewritten as $n(1 - e) - (1 - g) = 4k + 2n + y$. Thus $4k + 2n = 0$ so n is even and consequently $1 - g \in I_G^2$ so $g = 1$. □

(3.4) Remark. The converses of (1) and (2) in (3.3) are also true. Thus, for example, if p is odd, $G \to \bar{G}$ is an isomorphism, and the product $(\bar{G})(1 + (\mathbf{Z}p + \bar{M}^2)_{\text{tor}})$ is direct, then $K \subseteq \mathbf{Z}p + M^2$. To see this assume $x \in K$, say $x = np + (1 - g) + y$, $n \in \mathbf{Z}$, $g \in G$, $y \in I_G^2$. Then $\bar{g} = 1 + np + \bar{y}$ so by (3.1) $np + \bar{y}$ is torsion. Thus, by the directness of the product, $\bar{g} = \dot{1}$, so by the injectivity of $G \to \bar{G}$, $g = 1$. Thus $x = np + y \in \mathbf{Z}p + M^2$. The converse of (2) can be proved similarly, but the proof will not be given here.

References

[1] P. Berthelot, *Cohomologie Cristalline des Schèmas de Caractèristique p > 0*, Lecture Notes in Math., 407, Springer-Verlag, (1974).

[2] H. Cartan, *Sèminaire École Normale Supèrieure* 1954/1955: *Algèbres d'Eilenberg-MacLane et homotopie*, *Benjamin* (1967) (*Exposè* 7).

[3] R. Elman and T. Y. Lam, *Quadratic forms over formally real fields and Pythagorean fields*, Amer. J. Math., **94** (1972), 115–1194.

[4] J. L. Kleinstein and A. Rosenberg, *Succinct and representational Witt rings*, Pacific J. Math., **86** (1980), 99–137.

[5] M. Knebusch, A. Rosenberg, and R. Ware, *Structure rings and quotients of Abelian group rings*, Amer. J. Math., **94** (1972), 119–155.

[6] T. Y. Lam, *Ten Lectures on Quadratic Forms over Fields*, in *Conference on Quadratic Forms*–1976, Queen's Papers in Pure and Applied Math., **46** (1977).

[7] M. Marshall, *Abstract Witt Rings*, Queen's Papers in Pure and Applied Math., **57** (1980).

Received November 1, 1985

University of Saskatchewan
Saskatoon, Saskatchewan, Canada
S7N 0W0